M系列に基く一様乱数の多次元ランダムネスの検定(乱数プログラム・パッケージ)

AUTHOR(S):

山本, 英二; 菅野, 長武

CITATION:

山本, 英二 ...[et al]. M系列に基く一様乱数の多次元ランダムネスの検定(乱数プログラム・パッケージ). 数理解析研究所講究録 1983, 498: 182-190

ISSUE DATE:

1983-09

URL:

http://hdl.handle.net/2433/103630

数理解析研究所講究録
498巻 1983年 182-190

M系列に基く一様乱数の多次元ランダムネスの検定

園山理大　山本英二（Eiji Yamamoto）
林野高　菅野長武（Osamu Sugano）

1. M系列に基く一様乱数の発生法

周期Nの2値系列の内1周期では等頻度性や無系列相関性を持つ系列にM系列がある。M系列はその他にも良い性質を持つことが理論的に知られている。M系列を使って[0,1)の一様乱数を作る方法にTauswortheの法(1965)がある。彼の方法はP次の原始多項式を特性多項式とする漸化式を用いた周期$N=2^P-1$のM系列$\{a_i\}$を発生させ、その相続くℓ(≦P)個の要素を並べてℓビットの2進小数系列（これを横型系列という）を作るものである。

(1)　$$w_t = 0.a_{\sigma t+r-1}\, a_{\sigma t+r-2} \cdots a_{\sigma t+r-\ell}$$

（σ；≧ℓ, Nと素　r；初期位相）

このとき$\{w_t\}$は周期Nを持ち、k(≦$\frac{P}{\ell}$)次均等分布、平均・分散の不偏性や無系列相関性を高い精度で持つことが知

/

られている。　しかし，この方法は発生速度が遅い欠点を持つ。

この発生速度を高速化するために，M系列の位相をずらしたものを各ビットに配する縦型系列と呼ばれる2進小数系列

(2)　　$w_t = 0.a_{t+\tau_1} a_{t+\tau_2} \cdots a_{t+\tau_l}$

を発生させる Lewis & Payne 法(1973)や，その改良版 Arvillias & Maritsas 法(1978)が考案されたが彼らの系列は横型系列の持つ良い性質(k次均等分布)を失っていた。

そこで伏見・手塚(1981)，伏見(1983)は縦型系列の高速発生算法を利用して次の横型系列を発生させる方法を提案した。

3次原始多項式 $f(z) = z^{521} + z^{32} + 1$ を特性多項式とする漸化式

(3)　　$a_t \equiv a_{t-521} \oplus a_{t-32}$　　(⊕は繰り上りなしの和)

で作られる周期 $N = 2^{521} - 1$ のM系列に基づく横型系列は次の

(4)　　$w_t = 0.a_{32(t-1)+1}\, a_{32(t-1)+2} \cdots a_{32(t-1)+31}$

$(p=521,\ r=32,\ l=31,\ [p/l]=16)$

算法で発生させる。

1. $a_1, \cdots, a_{521}$ の値を任意に0又は1とする。(全て0とはしない)
2. (3)を用いて a_t $(t=522, \cdots, 16672)$ を発生させる。

3. (4) を用いて w_t ($t=1,\cdots,521$) を発生させる。

4. w_t ($t \geq 522$) を漸化式：

(5) $$w_t = w_{t-521} \oplus w_{t-32}$$

で発生する。

この算法は32とNが互いに素なので、M系列 $\{a_t\}$ を間隔32で抽出して得られる系列 $\{a_{32t}\}$ は元のM系列をある位相だけシフトしたものになっているので、初期位相を i とすれば

(6) $$a_{32t+i} = a_{32(t-521)+i} \oplus a_{32(t-32)+i} \quad (i=1,\cdots,31)$$

の漸化式が成り立つので (5) が成立することを利用したものである。

2. 統計的検定

伏見・千塚はこうして発生させた彼らのM系列に基く一様乱数は200万個の部分列についても多くの統計的検定項目：度数検定・系列検定・ポーカー検定・連の検定・ギャップの検定に合格すると報告している。1周期にわたればk次均等性を持つので部分列でもk次均等性の検定に合格すると思われるが、k次独立性についてはどうであろうか。そこで我々は伏見・千塚の一様乱数系列に2次元 d^2 検定，我々の提案した

3次元 Random Distance 検定(1981)，菅野の提案した4次元Random Manhattan Distance 検定(1982)を行った。即ち、

$$d_2^2 = \sum_{j=1}^{2} (U_{1j} - U_{2j})^2$$

(7) $$d_3^2 = \sum_{j=1}^{3} (U_{1j} - U_{2j})^2 \qquad \left(\begin{array}{l} \coprod (U_{ij}) \\ U_{ij} \sim U(0,1) \\ i=1,2 \;;\; j=1,\cdots,4 \end{array} \right)$$

$$MD_4 = \sum_{j=1}^{4} |U_{1j} - U_{2j}|$$

の分布を利用した検定である。 d_2^2, d_3^2 は2次元，3次元ベクトル空間の2点間のユークリッド距離の2乗である。MD_4 は4次元ベクトル空間の2点間のマンハッタン距離である。 d_4^2 が考えられるがその分布関数は初等関数の範囲で表現できない。 d_2^2, d_3^2, MD_4 の分布関数 F_2, F_3, F_4 は表1となる。 この分布関数を用いて χ^2 検定を行うことになる。

3、計算結果

ここでは伏見・手塚の報告(1981)と比較が可能となる様、彼らの発生させた一様乱数系列とまったく同一のものを用いた。

d_2^2-検定は、相続く千個の乱数で一つの d_2^2 を作りこれを500個使って一つの χ^2 値を計算した。 区間数は10とし、各区間がほぼ等確率0.1となるように区間端点は求めた。

このχ^2値を100個用いて次のKolmogorov－Smirnov検定統計量を計算した。

$$(8)\qquad \begin{aligned} KS+ &= \sup_t \{F_m(t) - F(t)\} \\ KS- &= \sup_t \{F(t) - F_m(t)\} \\ KS &= \sup_t |F_m(t) - F(t)| \end{aligned} \qquad \begin{pmatrix} F(t);\text{理論分布関数} \\ F_m(t);\text{経験分布関数} \end{pmatrix}$$

これを10回くり返した。使用乱数の数は $4\times500\times100\times10$ ＝200万個である。

d_3^2－検定は相続く6個の乱数で一つのd_3^2を作り、これを334個使って一つのχ^2値を計算する。区間数は10で、各区間、ほぼ等確率である。このχ^2値を100個用いてK－S検定統計量を計算した。これを10回くり返す。$6\times334\times100\times10$ ＝200.4万個の乱数を使用した。

MD_4－検定は相続く8個の乱数で一つのMD_4を作りこれを250個使って一つのχ^2値を計算する。区間数は同じ10である。等確率となるようにしておく。このχ^2値を100個用いてK－S検定統計量を計算する。これを10回くり返す。$8\times250\times100\times10$ ＝200万個の乱数を使用した。

計算結果が表2に示されている。d_2^3－検定のKS＋，d_2^3－検定のKS－で5%有意なものが10回中、各1回、MD_4－検定では5%有意なものがKS＋，KSで各10回中2回

でている。 MD_4ー検定では、不合格と言えそうである。伏見・手塚のM系列に基く一様乱数の200万個程の部分系列について、多次元ランダムネスについての統計的検定に不合格になる部分系列が存在するとの知見を得た。

REFERENCES

[1] R.C.Tauswerth(1965), Mathematics of Computation, 14, 201-209.

[2] T.G.Lewis & W.H.Payne(1973), J.ACM, 21, 456-468.

[3] A.C.Arvillias & D.G.Maritsas(1978), J.ACM, 25, 675-686.

[4] 伏見正則 & 手塚集(1981), 応用統計学, 10, 151-163.

[5] E.Yamamoto & O.Sugano(1981), J. Japan Statist. Soc., 11, 15-25.

[6] O.Sugano(1982), J. Japan Statist. Soc., 12,113-124.

[7] 伏見正則(1983), 情報処理, 24, 367-371.

表 1

$$F_2(\alpha^2)=\begin{cases}\pi\alpha^2-\dfrac{8}{3}\alpha^3+\dfrac{1}{2}\alpha^4 & (0\leqq\alpha^2\leqq1)\\[2ex] \dfrac{1}{3}+(\pi-2)\alpha^2+4(\alpha^2-1)^{1/2}+\dfrac{8}{3}(\alpha^2-1)^{3/2}-\dfrac{1}{2}\alpha^4-4\alpha^2\sec^{-1}\alpha & (1\leqq\alpha^2\leqq2).\end{cases}$$

$$F_3(\alpha^2)=\begin{cases}\dfrac{4}{3}\pi\alpha^3-\dfrac{3}{2}\pi\alpha^4+\dfrac{8}{5}\alpha^5-\dfrac{1}{6}\alpha^6, & (0\leqq\alpha^2\leqq1)\\[2ex] \left(\dfrac{5}{2}\pi+\dfrac{43}{30}\right)-6(\alpha^2-1)^{1/2}+\left(3\pi+\dfrac{7}{2}\right)(\alpha^2-1)-\dfrac{8}{3}\pi\alpha^3-10(\alpha^2-1)^{3/2}\\ \quad+\dfrac{5}{2}(\alpha^2-1)^2-\dfrac{16}{5}(\alpha^2-1)^{5/2}+\dfrac{1}{3}(\alpha^2-1)^3+6\alpha^4\sec^{-1}\alpha, & (1\leqq\alpha^2\leqq2)\\[2ex] \left(\dfrac{23}{2}\pi-\dfrac{343}{30}\right)+14(\alpha^2-2)^{1/2}+\left(9\pi-\dfrac{21}{2}\right)(\alpha^2-2)+10(\alpha^2-2)^{3/2}\\ \quad+\left(\dfrac{3\pi-5}{2}\right)(\alpha^2-2)^2+\dfrac{8}{5}(\alpha^2-2)^{5/2}-\dfrac{1}{6}(\alpha^2-2)^3\\ \quad-2(3\alpha^4+6\alpha^2-1)\sec^{-1}\sqrt{\alpha^2-1}+8\alpha^3\sec^{-1}(\alpha^2-1)-\dfrac{8}{3}\pi\alpha^3 & (2\leqq\alpha^2\leqq3).\end{cases}$$

$$F_4(x)=\begin{cases}0 & (\quad x\leq0)\\ 2x^4/3-8x^5/15+2x^6/15-4x^7/315+x^8/2520 & (0\leq x\leq1)\\ 641/2520+5(x-1)/7+37(x-1)^2/90-19(x-1)^3/45-5(x-1)^4/12\\ \quad+5(x-1)^5/9-19(x-1)^6/90+(x-1)^7/35-(x-1)^8/840 & (1\leq x\leq2)\\ 115/126+32(x-2)/105-2(x-2)^2/5+8(x-2)^3/45+(x-2)^4/9\\ \quad-8(x-2)^5/45+4(x-2)^6/45-2(x-2)^7/105+(x-2)^8/840 & (2\leq x\leq3)\\ 2519/2520+(x-3)/315-(x-3)^2/90+(x-3)^3/45-(x-3)^4/36\\ \quad+(x-3)^5/45-(x-3)^6/90+(x-3)^7/315-(x-3)^8/2520 & (3\leq x\leq4)\\ 1 & (4\leq x\quad).\end{cases}$$

表2

d_2^2-test

NO.	KS+	KS-	KS
1	.03362	.06147	.06147
2	.01841	.09032	.09032
3	.08069	.04155	.08069
4	.03325	.05084	.05084
5	.08597	.03126	.08597
6	.07982	.05318	.07982
7	.04177	.04314	.04314
8	.00819	.14688*	.14688*
9	.07130	.02157	.07130
10	.03642	.06422	.06422

d_3^2-test

NO.	KS+	KS-	KS
1	.02058	.08057	.08057
2	.12890*	.04410	.12890
3	.07869	.01146	.07869
4	.04691	.04684	.04691
5	.08452	.03011	.08452
6	.06874	.05620	.06874
7	.05353	.06379	.06379
8	.03924	.04565	.04565
9	.01309	.07439	.07439
10	.05776	.08293	.08293

MD_4-test

NO.	KS+	KS-	KS
1	.06708	.06241	.06708
2	.03183	.06278	.06278
3	.08216	.04143	.08216
4	.08638	.04165	.08638
5	.03336	.08364	.08364
6	.14487*	.01603	.14487*
7	.13908*	.00041	.13908*
8	.03075	.03361	.03361
9	.04434	.07716	.07716
10	.06521	.04623	.06521